Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

Guide relatif aux mesures techniques et organisationnelles de la protection des données

Août 2015

Feldeggweg 1, 3003 Berne
Tél. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Table des matières

INTRODUCTION GÉNÉRALE

Ce guide est proposé par le Préposé fédéral à la protection des données et à la transparence. Il constitue une introduction aux risques liés à la protection des données dans les systèmes d'information actuels. Il est conçu comme une aide pour la mise en œuvre de mesures adéquates dans le but d'assurer une protection optimale et appropriée des données personnelles. Les thèmes principaux de la protection des données sont présentés sous l'angle des mesures techniques et organisationnelles à mettre en place, comme le chiffrement, l'anonymisation, l'authentification, etc.

Ce guide est avant tout destiné aux personnes qui sont en charge des systèmes d'information, techniciens ou non, et qui sont confrontés directement au problème de la gestion des données personnelles. Mais toute personne qui s'intéresse à ces questions y trouvera des réponses.

Le guide est organisé autour de quatre thématiques : l'accès aux données, le cycle de vie des données, le transfert des données et le droit d'accès aux données. Pour chaque thématique, un certain nombre de points auxquels il faut veiller lors de la conception d'un système et de sa mise en œuvre sont soulevés. Pour chaque point, des mesures sont proposées. Elles doivent être comprises comme des lignes directrices générales et doivent être ensuite adaptées aux spécificités de chaque projet et de chaque organisation.

Définitions

Les termes suivants sont définis de manière précise afin d'assurer une bonne compréhension du guide.

Sécurité des données/informations

- La ***sécurité des données/informations*** regroupe toutes les mesures prises en vue d'assurer la confidentialité, l'intégrité et la disponibilité des données/informations.

Protection des données

- La ***protection des données*** regroupe toutes les mesures prises en vue d'éviter un traitement indésirable des données ainsi que les conséquences indésirables d'un traitement.

Protection de l'information

- La ***protection de l'information*** définit des niveaux de confidentialité pour l'information (INTERNE, CONFIDENTIEL, SECRET) dans la perspective de défendre les intérêts d'un pays ou d'une organisation.

Données personnelles

- Toutes les informations qui se rapportent à une personne identifiée ou identifiable sont des ***données personnelles***. On les qualifie de **données non sensibles**, lorsque celles-ci ne recèlent pas de sensibilité particulière (cf. définition ci-dessous).

- Les ***données sensibles*** sont des données personnelles qui se rapportent aux opinions ou activités religieuses, philosophiques, politiques ou syndicales, à la santé, à la sphère intime ou à l'appartenance à une race, à des mesures d'aide sociale, à des poursuites ou des sanctions pénales et administratives. Si la révélation de ces données peut entraîner des risques très élevés, en particulier liés à la vie de la personne concernée, on parle alors de ***données ultrasensibles*** (vitales).

- Un ***profil de la personnalité*** est un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne.

- La ***personne concernée*** est la personne à qui font référence des données personnelles.

- Quatre **niveaux de risque** s'appliquent aux données personnelles :

    1. ***risque minimal*** : données personnelles dont l'abus ne semble pas, en règle générale, avoir de conséquence particulière pour la personne concernée. Il s'agit par exemple du nom, du prénom, de l'adresse et de la date de naissance, pour autant qu'ils ne soient pas dans une relation sensible, ou alors d'informations qui apparaissent dans les médias.
    2. ***risque moyen*** : données personnelles dont l'abus peut affecter la situation économique ou la place dans la société de la personne concernée. Il s'agit par exemple de données relatives à la situation d'un locataire ou aux relations professionnelles.
    3. ***risque élevé*** : données personnelles dont l'abus peut gravement affecter la situation économique ou la place dans la société de la personne concernée. Il s'agit par exemple de données relatives à la santé d'un patient, de données sensibles ou de profils de la personnalité.
    4. ***risque très élevé*** : données personnelles dont l'abus peut mettre en danger la vie de la personne concernée. Il s'agit par exemple d'adresses d'hommes de liaison de la police, d'adresses de témoins dans certaines poursuites pénales ou d'adresses de personnes qui sont menacées suite à l'expression de leur opinion ou de leur appartenance religieuse ou politique.

Fichier

- Le droit suisse emploie le terme de ***fichier*** pour désigner une collection de données personnelles qui est organisée de façon à permettre une recherche par personne concernée parmi ces données.

Responsabilités

Les rôles suivants sont importants dans une organisation qui traite des données personnelles :

- Le ***maître du fichier*** est la personne ou l'organe fédéral qui décide du but et du contenu des données utilisées dans un système d'information.

- Le ***conseiller à la protection des données*** est la personne en charge, au sein d'une organisation, du conseil et du contrôle des traitements sous l'angle de la protection des données.

- Le ***préposé fédéral à la protection des données et à la transparence*** effectue des tâches de surveillance et de conseil auprès des personnes privées et des organes fédéraux. En outre, il tient et publie un registre des fichiers à déclaration obligatoire.

- Le ***préposé cantonal à la protection des données (et à la transparence)*** effectue des tâches similaires auprès des organes cantonaux et communaux.

Bases légales

La loi fédérale sur la protection des données (LPD) – en particulier l'art. 7 – et l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) – en particulier les articles 8 à 11 et 20 à 21 – sont les fondements de ce guide.

Mesures techniques et organisationnelles

Les mesures techniques et organisationnelles permettent de minimiser les risques liés à un système d'information. Ainsi, un système d'information qui contient des données personnelles doit respecter certains critères pour assurer la sécurité de ces données. La mise en œuvre de telles mesures permet d'agir dans ce sens.

Une mesure technique est directement liée au système d'information lui-même et le concerne directement. Une mesure organisationnelle se rapporte plus à l'entourage du système, en particulier aux personnes qui l'utilisent.

Les deux types de mesures sont indispensables. C'est de manière combinée qu'elles permettent d'éviter la destruction et la perte des données, ainsi que les erreurs, la falsification, les accès non autorisés, etc. Ces mesures s'inscrivent dans le cycle de vie d'un système d'information et sont appliquées à tous les niveaux du système.

Le schéma 1 ci-après donne un aperçu du cycle de vie d'un système d'information. Il illustre comment les données sont introduites, traitées, communiquées, sauvegardées, etc. et indique également à quels niveaux des tiers peuvent intervenir, que ce soient des collaborateurs, des tiers traitants ou les personnes concernées par les données du système.

Contenu du guide

Quatre thématiques sont extraites du schéma 1 et donnent les lignes directrices de ce guide. Nous traitons ainsi des mesures techniques et organisationnelles liées à (1) l'accès aux données, (2) le cycle de vie des données, (3) le transfert des données et (4) le droit d'accès aux données.

Pour chaque thématique, différents aspects sont abordés et les mesures associées sont présentées. Pour chaque aspect, nous soulignons quelques bonnes pratiques qui sont autant de conseils pour le développement d'applications respectueuses de la sphère privée. Il est évident que ces mesures doivent être adaptées à la sensibilité des données, à la nature des traitements, à l'étendue de l'information utilisée, etc.

En conclusion, nous indiquons des outils existants qui permettent d'anticiper les risques liés à la protection des données ou de décrire formellement les mesures mises en place.

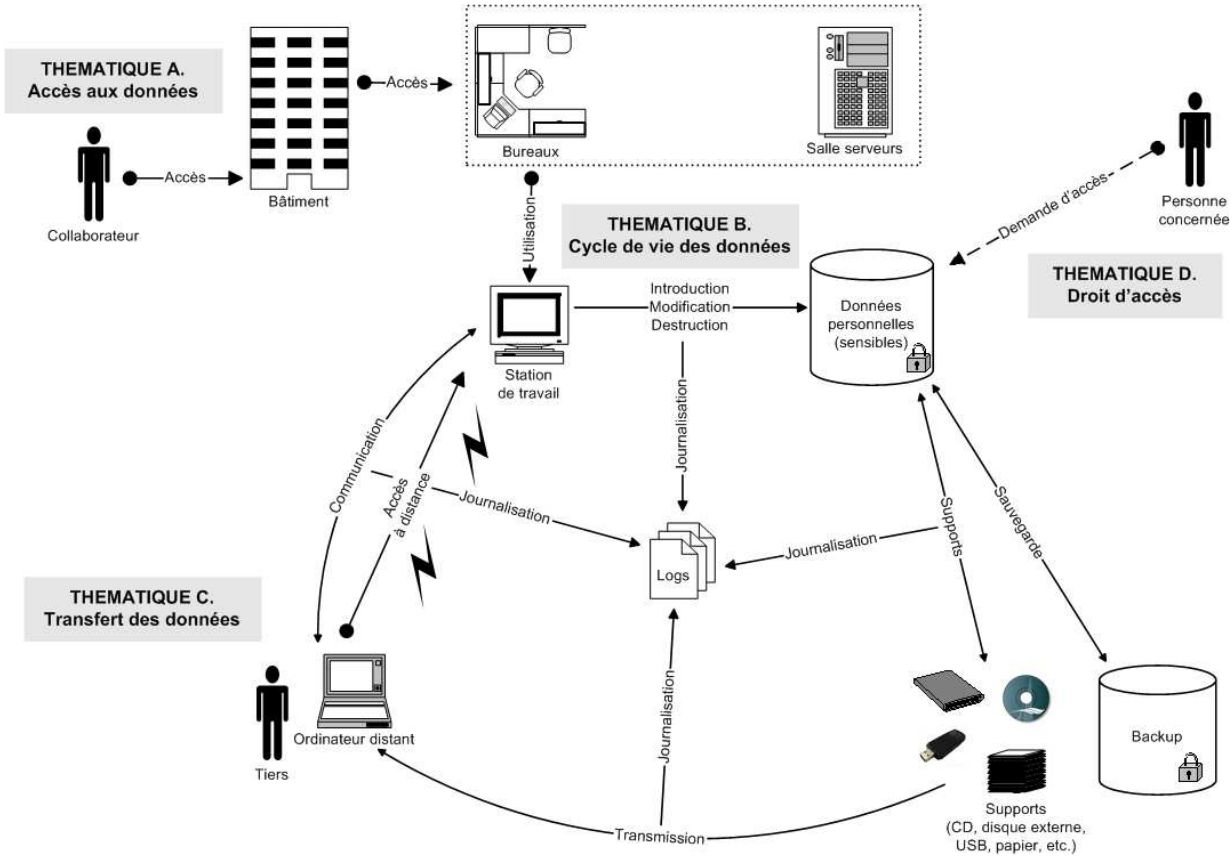


Schéma 1. Vue d'ensemble de l'application des mesures techniques et organisationnelles. Chaque partie est commentée par thématique dans les différents chapitres du guide.

THÉMATIQUE A. L'ACCÈS AUX DONNÉES

La première thématique concerne l'accès aux données par les différents utilisateurs du système. L'accès aux données doit être traité sous plusieurs angles. Ainsi, l'emplacement physique des données doit être précisément étudié : où se trouvent les serveurs de données et comment assurer leur sécurité en tenant compte de tous les acteurs impliqués ? Ensuite, il faut déterminer la manière dont ces données peuvent être consultées, modifiées, etc. Ceci implique plusieurs niveaux de sécurité : les ordinateurs qu'utilisent les collaborateurs doivent être accessibles aux seules personnes à qui l'on décide d'accorder un accès et protégés contre les tentatives d'intrusion extérieure. Ces tentatives peuvent être locales – une personne non autorisée pénètre dans les locaux – ou distantes – une personne non autorisée accède au système à travers le réseau. Finalement, il faut décider de la trace que l'on souhaite conserver des accès physiques et électroniques.

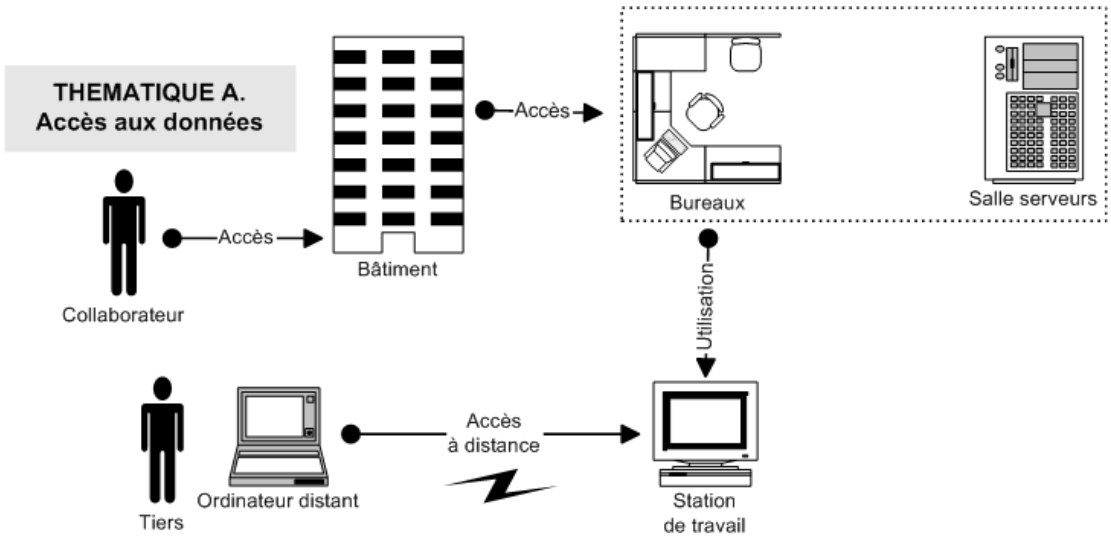


Schéma A. *L'accès aux données*

Le schéma A évoque les questions suivantes qui sont traitées en détails et accompagnées de mesures concrètes.

A.1 Comment assurer la sécurité des locaux ?
A.2 Comment assurer la sécurité des serveurs ?
A.3 Comment assurer la sécurité des places de travail ?
A.4 Comment assurer l'identification et l'authentification des utilisateurs ?
A.5 Comment sécuriser l'accès aux données des utilisateurs ?
A.6 Comment gérer les accès à distance ?

A.1 Sécurité des locaux

Les locaux sont définis comme les lieux où les utilisateurs du système travaillent et, par conséquent, ont accès aux données. Les données sont physiquement stockées dans les salles de serveurs (cf. section A.2 – Sécurité des salles de serveurs) et les ordinateurs personnels sont des périphériques qui permettent d'accéder à ces données. L'accès à ces machines, en tant qu'interfaces vers les données, doit être contrôlé. Seules les personnes autorisées doivent accéder aux bâtiments et aux bureaux. Les fonctions de ces personnes peuvent être variées et il faut toutes les prendre en compte pour définir des droits d'accès spécifiques : les collaborateurs de l'organisation en font partie, évidemment, mais également le personnel de maintenance, de nettoyage, etc.

Il faut tenir compte du contexte global pour prendre les mesures adéquates. Si plusieurs organisations partagent un même bâtiment, elles n'ont pas les mêmes besoins en matière de protection des données. Alors la sécurité doit être adaptée, par étage par exemple. De plus, les serveurs de données peuvent être externalisés et leur sécurité par conséquent confiée à des tiers.

Mesures à envisager

- L'accès au(x) bâtiment(s) est réglementé. Un badge, éventuellement associé à un code d'accès, permet l'authentification des personnes qui souhaitent entrer dans le bâtiment.
- Si plusieurs organisations partagent le même bâtiment, il faut, si nécessaire, également réglementé l'accès aux locaux de l'organisation d'une manière similaire : un système d'accès électronique est installé à l'étage ou dans la section réservée à l'organisation.
- Une réglementation particulière ainsi qu'une procédure d'accueil pour les visiteurs est établie afin d'éviter qu'ils se déplacent seuls et librement dans le bâtiment.
- Les bureaux sont verrouillés en dehors des heures de présence.
- Des alarmes sont éventuellement placées dans les locaux les plus sensibles et sont activées en dehors des heures de présence.

A.2 Sécurité des salles de serveurs

Les salles de serveurs sont les lieux les plus sensibles d'une organisation puisque les données sont physiquement stockées sur ces machines. L'intégrité et la disponibilité des données sont garanties si la perte définitive des données est impossible grâce à la mise en place de mesures appropriées. Il est important de déterminer là aussi qui est autorisé à accéder à ces salles. Avec un nombre restreint d'autorisations accordées, la sécurité est

améliorée. Il faut éviter de mauvaises manipulations sur les serveurs, intentionnelles ou non, qui mènent à une destruction ou une modification des données. Ainsi, des mesures particulières doivent être prises pour sécuriser les salles de serveurs.

Mesures à envisager

- Un nombre restreint de personnes est autorisé à pénétrer dans les salles de serveurs. Autoriser l'accès à toutes les personnes qui partagent une fonction identique est trop laxiste. L'accès à des fins de maintenance des systèmes est autorisé à un nombre restreint de techniciens. De même, il est judicieux de toujours confier le nettoyage des salles aux mêmes employés.

- Les accès aux salles de serveurs sont journalisés.

- Une alarme est installée et fonctionne en continu pour éviter toute intrusion frauduleuse.

- Idéalement, la salle de serveurs se trouve au sous-sol afin de minimiser le nombre d'accès physiques (portes, fenêtres, etc.)

- Les incidents naturels, tels que les incendies ou les inondations, sont détectables de manière automatique et signalés par des alarmes.

A.3 Sécurité des places de travail

Les collaborateurs accèdent et traitent les données depuis leur place de travail. L'ordinateur personnel du collaborateur y est installé. L'environnement de travail doit être sécurisé par une disposition stratégique des différents périphériques. Un nombre suffisant de rangements qui peuvent être fermés à clé doit être mis à disposition du collaborateur.

L'ordinateur personnel doit être protégé par un mot de passe connu du collaborateur seul. Il doit également être protégé par les logiciels nécessaires pour éviter les intrusions. La protection doit couvrir tous les types de virus, de logiciels malveillants (malwares) et d'attaques au sens large.

Mesures à envisager

- Les places de travail sont aménagées de telle sorte que les écrans d'ordinateurs ne sont pas visibles depuis la porte. Les visiteurs, extérieurs à l'organisation, ne peuvent ainsi pas observer le travail des collaborateurs.

- Les documents imprimés ne restent pas sans surveillance autour de l'imprimante. Par exemple, le collaborateur introduit un code dans l'imprimante pour libérer l'impression de ses documents.

- Le collaborateur dépose ses documents imprimés et tout le matériel sensible (clés USB, CD-ROM, etc.) dans des rangements qu'il peut fermer à clé.

- Les ordinateurs portables, éventuellement les ordinateurs fixes également, sont enchaînés au bureau afin d'éviter les vols à l'intérieur des locaux.

- Un logiciel antivirus est disponible et activé sur toutes les machines. Il est mis à jour régulièrement.

A.4 Identification et authentification

L'identification permet de connaître l'identité d'un individu, de le distinguer parmi d'autres.

L'authentification permet de vérifier qu'un individu est bien celui qu'il prétend être. L'authentification se fait à l'aide de preuves que l'individu présente au système. Ces preuves sont de trois types. Il peut s'agir d'un objet que l'individu *possède* (un badge par exemple) ou d'une information que l'individu *connaît* (un mot de passe par exemple) ou alors d'une *propriété qui caractérise* l'individu (une propriété comportementale, telle que la signature, ou une propriété morphologique telle qu'une empreinte digitale). On parle d'authentification forte quand au moins deux modalités sont combinées (badge et mot de passe par exemple).

Ainsi, l'authentification est utilisée pour permettre aux utilisateurs de pénétrer dans les locaux et d'accéder aux données en se connectant à leur ordinateur. L'identification permet de reconnaître l'individu qui a introduit, modifié ou détruit des données dans le système à un moment donné.

L'authentification unique (SSO, Single Sign-On) est une méthode qui permet à l'utilisateur d'accéder à plusieurs applications en ne procédant qu'à une seule authentification.

Mesures à envisager

- Les comptes utilisateurs qui permettent l'authentification sont uniques. Les collaborateurs ne partagent pas de compte. Un compte comprend un identifiant (nom d'utilisateur) associé à un mot de passe, ou un badge, etc.

- Idéalement, chaque individu possède des comptes différents pour s'authentifier sur sa machine de travail puis sur les différentes applications qu'il utilise. Ainsi, si une personne mal intentionnée accède à la machine, elle n'est pas encore en mesure d'accéder aux données par le biais des applications installées.

- Si une authentification unique est utilisée (SSO), les mesures de sécurité sont adaptées puisque, grâce à ce mécanisme, l'accès à la machine autorise également l'accès aux applications.

- Le mot de passe doit être fort et changé régulièrement. Un mot de passe fort contient au minimum 8 caractères dont des lettres (majuscules et minuscules), des chiffres et des caractères spéciaux !

- La fréquence de changement du mot de passe est inversement proportionnelle à la complexité exigée pour celui-ci.

- L'authentification à l'aide de données biométriques doit être réalisée dans le respect des mesures présentées dans le « Guide relatif aux systèmes de reconnaissance biométrique »[1].

A.5 Accès aux données

Toutes les données sont stockées sur les serveurs centraux. La plupart des collaborateurs n'ont pas la nécessité d'avoir accès à l'ensemble des données. En restreignant l'accès aux seules données utiles à chaque collaborateur, les risques d'une mauvaise utilisation des données – volontaire ou non – sont diminués. Les abus peuvent également être prévenus. Des règles d'accès et un mécanisme d'autorisation doivent donc être définis par rapport aux fonctions de chaque collaborateur.

Mesures à envisager

- Le système d'information est organisé de telle manière que des accès différenciés puissent être accordés aux utilisateurs.

- L'organisation interne définit les droits d'accès de chaque collaborateur en élaborant une matrice des droits d'accès.

- Le collaborateur s'authentifie à la mise en marche du système. Plus la sensibilité des données qu'il traite est grande, plus l'authentification est forte.

- Une journalisation est effectuée sur les accès au système suivant les conditions abordées à la section B2 – Journalisation.

A.6 Accès à distance

Les accès à distance peuvent être de plusieurs types et des mesures de protection doivent être envisagées pour chaque situation distincte.

Un accès aux données peut être demandé par un collaborateur qui souhaite travailler depuis l'extérieur et souhaite un accès distant à son ordinateur du bureau. Suivant la politique de

[1] www.leprepose.ch > Thèmes > Protection des données > Biométrie

l'organisation et la sensibilité des données, ce type d'accès doit être réglementé. Une méthode sûre d'authentification doit être mise en place. L'accès aux données peut aussi être demandé par un tiers autorisé, comme un sous-traitant, par exemple. Le cas doit être clairement réglé et une authentification forte doit être requise. Finalement, avant toutes choses, ce sont les accès frauduleux qui doivent être absolument évités.

La section C.1 – Sécurité du réseau – apporte des compléments en matière de sécurité des communications entre un tiers distant et l'organisation.

Mesures à envisager

- Un accès sécurisé est proposé aux personnes qui souhaitent ou doivent se connecter à distance.
- La méthode d'authentification choisie est forte et donc composée de deux modalités au moins.
- Les ordinateurs personnels sont protégés par un pare-feu (firewall).
- Sous les conditions abordées à la section B2 – Journalisation, les accès peuvent être journalisés.

THÉMATIQUE B. LE CYCLE DE VIE DES DONNÉES

Avec la mise en œuvre des mesures précédentes, l'accès aux données peut être considéré comme sûr, tant du point de vue physique (accès aux serveurs centraux) que du point de vue du traitement (accès aux ordinateurs personnels). La phase suivante consiste à assurer la sécurité des données durant leur cycle de vie. Elles doivent rester intègres et fiables durant l'entier de ce cycle, c'est-à-dire depuis leur introduction dans le système jusqu'à leur destruction, leur anonymisation ou leur archivage, en incluant évidemment toutes les phases de traitement qu'elles vont subir.
Les traitements peuvent être effectués au sein de l'organisation par les collaborateurs autorisés. Toutefois, ils peuvent également être sous-traités dans des organisations tierces.
De plus, dans le cadre des traitements, les données sont régulièrement transférées sur des supports mobiles, tels que des clés USB, des disques durs externes, etc. Finalement, garder une trace des différents traitements permet, en cas de problèmes, de mieux comprendre d'où ils proviennent.
Tous ces aspects et situations doivent être étudiés afin d'éviter des abus.

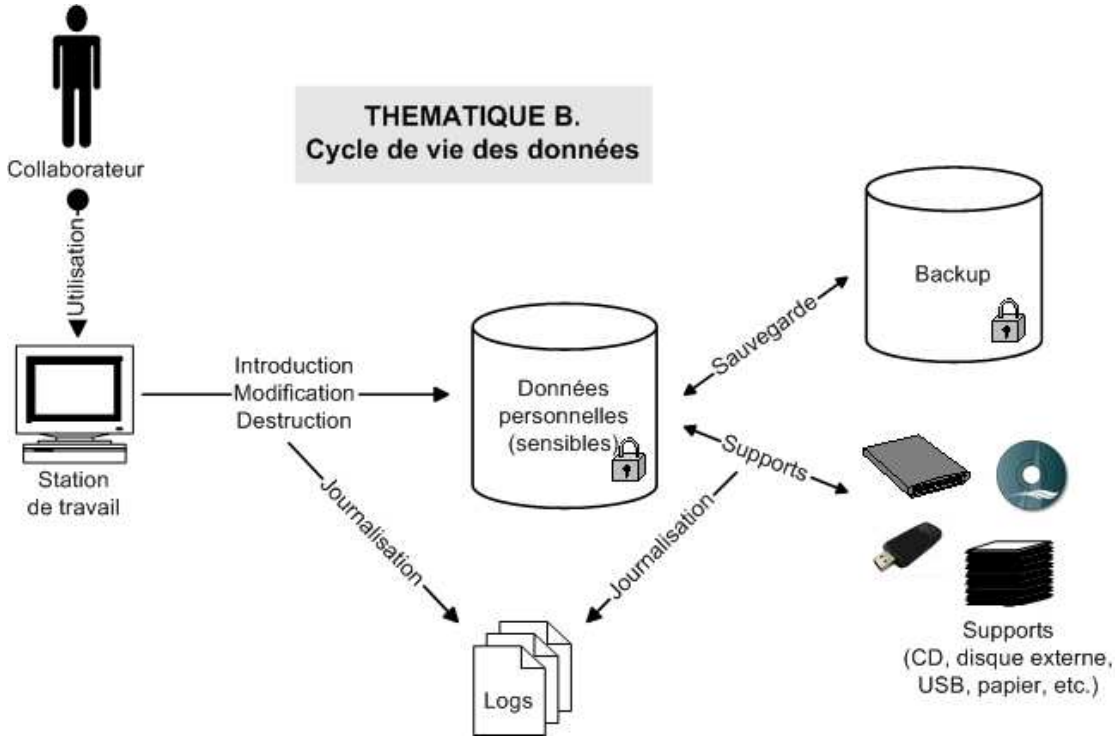


Schéma B. *Le cycle de vie des données*

Pour cette thématique, nous abordons les questions suivantes illustrées dans le schéma B :

B.1 Comment gérer l'introduction des données dans le système ?
B.2 Comment surveiller les traitements sur les données (journalisation) ?
B.3 Comment pseudonymiser et/ou anonymiser les données ?
B.4 Comment chiffrer les données ?
B.5 Comment assurer la sécurité des différents supports de données ?
B.6 Comment assurer la sauvegarde les données ?
B.7 Comment détruire de manière définitive les données ?
B.8 Comment gérer la sous-traitance de projets ?
B.9 Comment gérer la sécurité de l'information et la protection des données ?

B.1 Introduction des données

L'introduction de données dans le système est une étape délicate puisqu'il s'agit d'éviter à tout prix d'introduire dans le système des données incomplètes ou erronées. Une fois les données dans le système, les traitements qui seront effectuées sur cette base pourraient conduire à des résultats fallacieux et des décisions non appropriées. Il est important de développer des mécanismes d'aide pour minimiser les risques d'erreur lors de la saisie des données par les collaborateurs. De plus, il faut distinguer l'introduction de données dans un système en phase de test et l'introduction des données réelles.

Mesures à envisager

- Les données sont introduites uniquement par du personnel formé et autorisé.
- Des mécanismes d'aide sont mis en place dans le système. Le système repère les informations manquantes et effectue éventuellement des tests de vraisemblance sur les saisies.
- Les données utilisées pour les tests sont soit des données fictives, soit des données anonymisées.
- Selon les règles introduites dans la section B2 – Journalisation, il est possible de journaliser l'introduction des données.

B.2 Journalisation

Il est parfois utile de garder une trace de tous les traitements effectués sur les données. Il peut s'agir de l'introduction de nouvelles données, de modifications de données existantes ou de la destruction de données. En conservant une trace de ces différentes actions, il est possible, en cas de problèmes, de remonter à la source d'un incident, d'un accès frauduleux ou d'un traitement non autorisé sur les données. Les actions peuvent être journalisées : un enregistrement séquentiel de tous les événements qui sont liés au système d'informations est effectué et ces fichiers de « logs » (ou journaux) sont conservés pour un intervalle de temps proportionnel à la sensibilité des données et des traitements.

Les accès aux données, l'introduction de nouvelles données, la modification, la destruction, etc. peuvent être journalisés. Toutefois, la journalisation n'est *obligatoire* que dans le cas où les données traitées sont des données sensibles et que les mesures préventives mises en place ne sont pas suffisantes pour assurer la sécurité des données.

Dans les autres cas, un mécanisme de journalisation peut être intégré au système. La nécessité de cette journalisation doit être claire et associée à des buts précis. De plus, la journalisation doit être proportionnelle en termes de quantité d'informations journalisées et de durée de conservation des fichiers de logs.

Mesures à envisager

- Une argumentation précise soutient la mise en place d'un mécanisme de journalisation.
- Le contenu des fichiers de logs et la durée de conservation de ces fichiers sont proportionnels aux données et aux traitements effectués.
- Les collaborateurs sont informés qu'une trace des actions qu'ils effectuent sur les données est conservée.
- Les fichiers issus de la journalisation (journaux) sont sécurisés.
- Les droits d'accès sur les journaux sont clairement définis et limités à certaines fonctions au sein de l'organisation.
- Le mécanisme est protégé contre des éventuelles attaques ou des accès frauduleux qui auraient pour but de modifier le contenu des journaux.

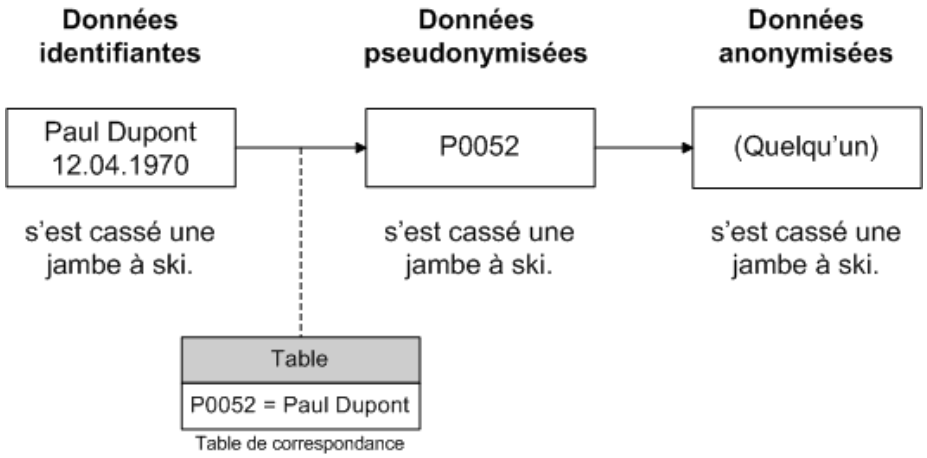
B.3 Pseudonymisation et anonymisation

Pour éviter que les personnes dont les données personnelles sont traitées dans le système puissent être identifiées, il est nécessaire de pseudonymiser ou d'anonymiser les données. La pseudonymisation consiste à remplacer l'ensemble des données identifiantes par un identifiant neutre (pseudonyme), tandis que l'anonymisation consiste à supprimer définitivement toutes les données identifiantes ou tout moyen de retrouver les données originales. La pseudonymisation est réversible tandis que l'anonymisation est définitive. De plus, des données parfaitement anonymisées ne sont plus considérées comme des données personnelles.

Les données identifiantes permettent d'identifier la personne sans difficulté. Ensuite une table de correspondance est utilisée pour faire le lien entre le pseudonyme et les données identifiantes d'une personne. Tant que la table de correspondance existe et est accessible, la pseudonymisation est une opération réversible. La dernière étape consiste à détruire de manière définitive toutes les données identifiantes (par exemple, il est possible de détruire la

table de correspondance). La personne n'est plus identifiable d'aucune manière et l'opération est irréversible.

Le schéma suivant donne un aperçu de ce processus :



Mesures à envisager

- Il faut privilégier l'utilisation de données anonymisées dans les limites des possibilités du projet. Si les données sont anonymisées, alors la loi sur la protection des données ne s'applique plus et la plupart des mesures présentées dans ce guide n'ont plus à être appliquées.

- En cas de pseudonymisation ou d'anonymisation, aucune information identifiante indirecte n'est conservée. On obtient une information identifiante indirecte lorsque la mise en relation de certaines informations qui, prises séparément, ne sont pas significatives permet d'identifier une personne.

- Si l'anonymisation n'est pas envisageable, les collaborateurs travaillent si possible sur des données pseudonymisées.

- La table de correspondance doit être sécurisée. Ainsi, elle ne doit être accessible qu'à un nombre restreint de collaborateurs et si possible être chiffrée.

- Si la pseudonymisation n'est pas envisageable, alors les collaborateurs travaillent sur des données nominatives. Si ces données sont sensibles, elles doivent être mémorisées sous forme chiffrée (cf. section B.4 Chiffrement des données).

B.4 Chiffrement des données

Les données sont habituellement mémorisées sur un disque dur sous forme de fichiers ou dans une base de données. Une méthode pour protéger les données personnelles et éviter qu'elles ne soient lues et modifiées de manière abusive consiste à chiffrer ces données. À l'aide d'une clé, les données sont transformées en un code non compréhensible. Ainsi, le chiffrement rend les données inintelligibles pour celui qui ne possède ou ne connaît pas la clé.
Dans la thématique suivante (C. La transmission des données), nous abordons le problématique du transfert de données dont les risques peuvent être réduits grâce à un chiffrement adapté.

Mesures à envisager

- L'algorithme de chiffrement et plus particulièrement la longueur de la clé sont proportionnels à la sensibilité des données.
- Sur un même support de données, différents groupes de données peuvent être chiffrés avec des clés propres.
- Les clés de chiffrement sont sécurisées.
- L'accès aux clés est limité à un nombre restreint de collaborateurs.

B.5 Sécurité des supports

Les données ne sont pas seulement mémorisées sur les serveurs centraux et les ordinateurs personnels. De nombreux supports externes permettent de transférer de l'information entre collaborateurs ou vers l'extérieur sans avoir à passer par le réseau. Des sauvegardes temporaires et limitées sont également possibles sur ces supports.
Parmi les supports externes, les clés USB, les disques durs externes, les CD-ROM, etc. ont des fonctions diverses puisqu'ils n'ont pas tous les mêmes propriétés. Certains sont réinscriptibles, comme les clés USB, d'autres ne le sont pas, comme les CD-ROM. Il est possible de stocker une quantité de données toujours plus importante sur un support visiblement toujours plus petit. Il faut garder cela à l'esprit pour éviter de minimiser les risques liés à ces supports.

Mesures à envisager

- Les collaborateurs sont formés aux dangers d'introduire un support inconnu (clé USB) dans son ordinateur.
- Les supports externes contenant des données personnelles sensibles ou des profils de personnalité sont chiffrés.

- Les supports externes doivent être mis sous clé.
- Une procédure de destruction des supports est mise en place et les outils nécessaires à cette destruction sont disponibles.

B.6 Sauvegarde des données

Il est essentiel d'assurer l'intégrité et la disponibilité des données contenues dans le système. Il faut donc définir une procédure pour la sauvegarde des données. Ainsi, si les données sont détruites à la suite d'une mauvaise utilisation ou d'un traitement frauduleux ou si elles sont corrompues, il doit être possible de les récupérer dans l'état le plus récent possible. Les intervalles de sauvegarde doivent être proportionnels à la quantité de traitements effectués journellement sur les données.

Mesures à envisager

- Une stratégie de sauvegarde est définie de manière appropriée en fonction des données elles-mêmes, de leur quantité et de leur fréquence de modification.
- La stratégie de sauvegarde est communiquée aux collaborateurs.
- Les serveurs de sauvegarde doivent être soumis aux mêmes mesures de sécurité que les serveurs centraux.
- La récupération des données est effectuée par du personnel formé à cette tâche.

B.7 Destruction des données

Les données personnelles n'ont pas pour vocation d'être conservées sans aucune limite de temps. Leur durée de conservation doit être définie et des mécanismes pour la destruction définitive de ces données doivent être établis. Ainsi, il ne suffit pas d'effacer simplement ses données d'un disque dur pour considérer qu'elles sont détruites. Il faut véritablement assurer qu'elles ne seront plus jamais accessibles. Il en va de même pour les données qui sont contenues sur papier ou sur des supports mobiles. Les copies de sauvegardes doivent également être détruites.

Mesures à envisager

- Les données papier sont détruites par une déchiqueteuse de papier.
- Les CD-ROM et autres supports mobiles sont également détruits physiquement.
- Les données sont effacées à l'aide de programmes spéciaux qui garantissent un effacement physique et définitif des données.

B.8 Sous-traitance (traitement par des tiers)

Il arrive régulièrement qu'une organisation sous-traite une partie de ses projets. Il peut s'agir du développement du projet, de la maintenance d'un système, de la sauvegarde des données, etc., qui sont confiés à des entreprises tierces. L'organisation qui fournit le mandat doit s'assurer que des règles équivalentes aux siennes en matière de protection des données sont appliquées par le sous-traitant. En tant que mandataire, l'organisation est responsable de ses données.

Mesures à envisager

- Le contrat avec le sous-traitant respecte les règles de l'organisation en charge du projet.
- L'organisation s'assure régulièrement que les conditions de protection des données sont respectées.
- La transmission des données entre le sous-traitant et l'organisation est réglementée.

B.9 Sécurité et protection

Pour sécuriser les données de manière optimale, il faut mettre en relation la nature des données personnelles (non sensibles, sensibles ou "ultrasensibles", selon les définitions du chapitre introductif) liée au niveau de risque (minimal, moyen, élevé, très élevé) et la classification de l'information (INTERNE, CONFIDENTIEL, SECRET). Il est possible d'établir la matrice suivante afin de définir des niveaux de protection adaptés aux deux échelles de classification. La mesure la moins contraignante s'applique à tous les niveaux supérieurs.

Prot. données / Prot. info.	Données non personnelles	Données personnelles non sensibles	Données personnelles sensibles	Données personnelles "ultrasensibles"
	Risque :	minimal/moyen	élevé	très élevé
Information non classifiée		**Protéger l'accès**	Protéger **+ Chiffrer** **+ Journaliser le traitement**	Protéger Chiffrer Journaliser **+ Numéroter (*)**
Information INTERNE	**Protéger l'accès**	Protéger	Protéger Chiffrer Journaliser	Protéger Chiffrer Journaliser Numéroter
Information CONFIDENTIELLE	Protéger **+ Chiffrer**	Protéger Chiffrer	Protéger Chiffrer Journaliser	Protéger Chiffrer Journaliser Numéroter
Information SECRÈTE	Protéger Chiffrer **+ Numéroter (*)**	Protéger Chiffrer Numéroter	Protéger Chiffrer Journaliser Numéroter	Protéger Chiffrer Journaliser Numéroter

(*) La numérotation des copies du document est une mesure en relation avec la protection de l'information.

Mesures

- Le système est élaboré en fonction des critères de la matrice ci-dessus.
- En fonction de la matrice ci-dessus, les mesures adéquates sont mises en place.

THÉMATIQUE C. LE TRANSFERT DES DONNÉES

Les moyens de communications actuels permettent de travailler à distance, d'échanger de l'information facilement et rapidement. Ainsi, les données ne restent plus simplement à l'intérieur de l'organisation mais sont souvent transmises à l'extérieur. Des contacts avec des tiers sont réguliers. La protection des données, durant leur transfert, doit également être garantie.

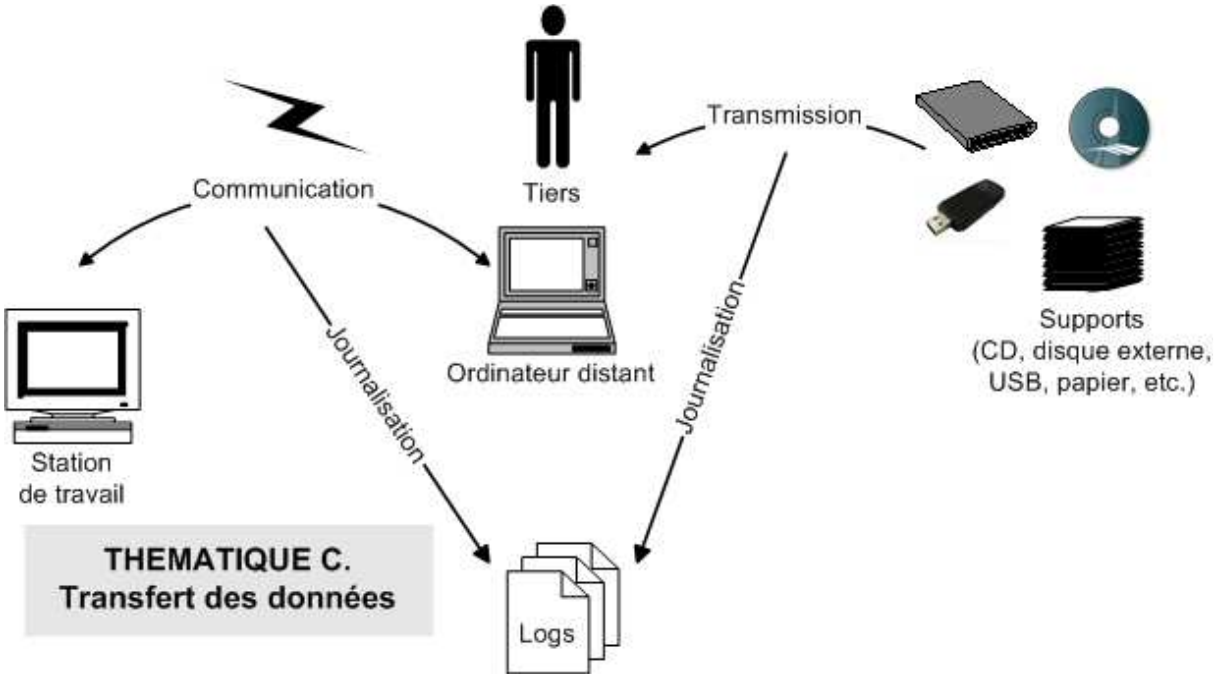


Schéma C. *Le transfert des données*

Sur la base du schéma C, nous abordons les questions suivantes :

C.1 Comment assurer la sécurité ?
C.2 Comment chiffrer un message que l'on envoie à avec un tiers distant ?
C.3 Comment signer un message que l'on envoie à un tiers distant ?
C.4 Comment transmettre les supports mobiles de manière sécurisée ?
C.5 Comment garder trace des différentes communications ?

C.1 Sécurité du réseau

Les communications au réseau interne d'une organisation sont nombreuses. Il peut s'agir de collaborateurs qui travaillent à distance et souhaitent se connecter au réseau interne ou de tiers qui accèdent aux données par ce biais. La sécurité du réseau et des communications doit être garantie. Les accès se font généralement via Internet. Il est donc indispensable d'utiliser des protocoles de communication sécurisés. Le protocole TLS (Transport Layer Security), successeur de SSL (Secure Sockets Layer), permet d'établir un canal de communication chiffré sécurisé entre un client et un serveur. Les algorithmes et les clés cryptographiques sont négociés entre le client et le serveur. TLS permet également aux deux parties de s'authentifier à l'aide de certificats. Ce protocole est une sous-couche des protocoles de communications usuels (HTTP, FTP, etc.). Il est transparent pour l'utilisateur et son utilisation peut être remarquée par l'apparition d'un cadenas fermé dans la fenêtre de la plupart des navigateurs.

De plus, la mise en place de connexions VPN (Virtual Private Network – réseau privé virtuel) permet de sécuriser l'accès au réseau interne. Il permet d'encapsuler les données chiffrées à transmettre. Un réseau VPN est basé sur des protocoles cryptographiques forts, tels que TLS, IPSec ou SSTP.

Mesures à envisager

- Les communications via Internet du réseau interne vers l'extérieur doivent être limitées au strict nécessaire.
- Il faut étudier si la mise en place d'un protocole de communication sécurisé (TLS) est nécessaire au vu des traitements à effectuer sur les données et le cas échéant, le mettre en place.
- Il faut mettre en place un VPN si des collaborateurs ou des tiers sont amenés à se connecter à distance au réseau local de l'organisation.

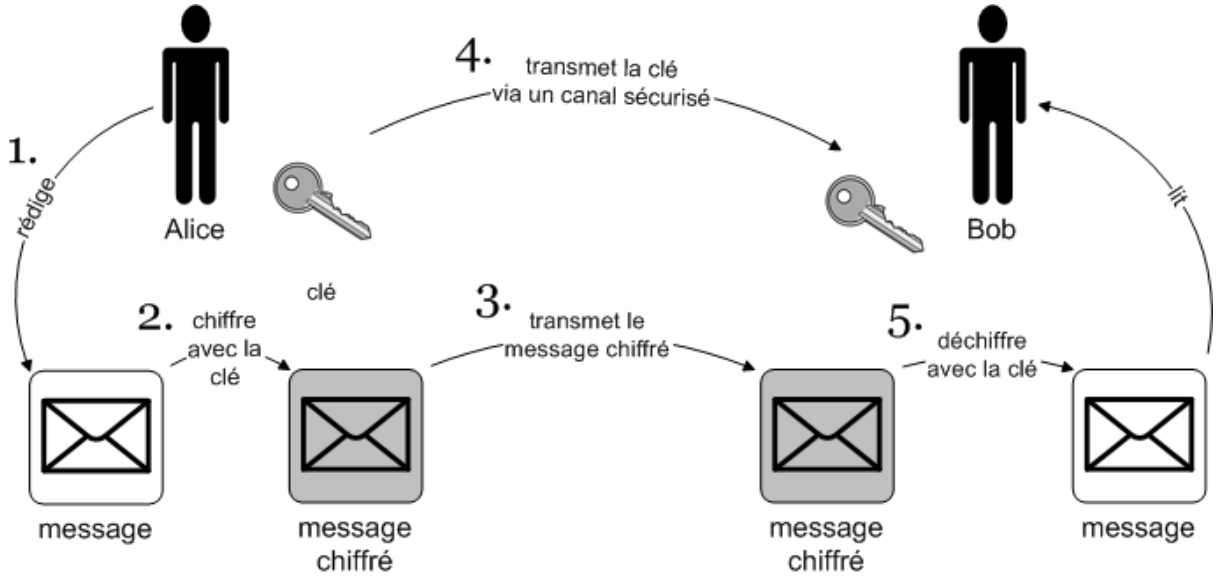
C.2 Chiffrement des messages

Parallèlement au chiffrement des disques durs et des fichiers pour empêcher les accès indésirables aux données, il est nécessaire de chiffrer les messages afin d'éviter qu'une tierce partie qui écoute la communication soit en mesure de lire, de modifier ou de supprimer le message.

Il existe deux méthodes pour le chiffrement de message, il s'agit du chiffrement symétrique et du chiffrement asymétrique.

Le chiffrement symétrique fonctionne selon le schéma ci-dessous :

1. Alice rédige un message pour Bob.
2. Alice chiffre son message au moyen d'une clé.
3. Alice transmet le message chiffré à Bob.
4. Alice transmet la clé à Bob de manière sécurisée.
5. Bob utilise cette clé pour déchiffrer le message.

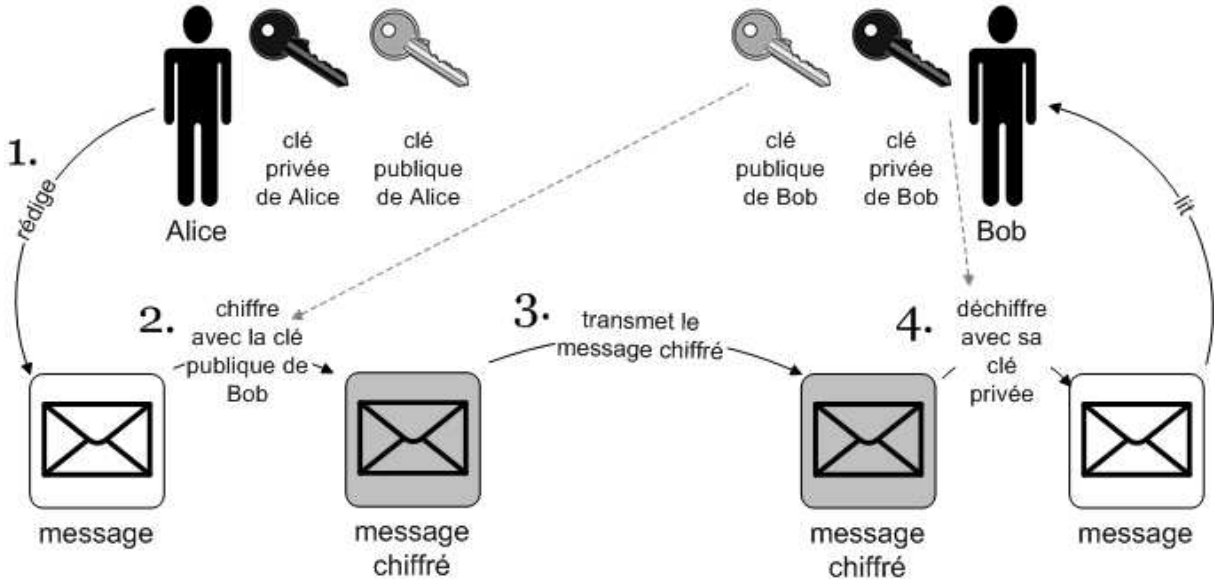


Le chiffrement symétrique est plus simple à mettre en œuvre car il ne comprend qu'une seule clé. Toutefois, la transmission de cette clé doit être effectuée de manière sûre.

Le chiffrement asymétrique est plus complexe mais il évite les problèmes liés à la transmission de la clé. Ce n'est pas une clé qui est utilisé mais deux. Chaque utilisateur génère une paire de clés : l'une est publique et rendue disponible à tous, la seconde est privée et connue de l'utilisateur seulement. La clé publique est utilisée pour chiffrer le message et la clé privée pour le déchiffrer. Cette technique permet également de signer les messages (cf. section C.3 Signature des messages).

Le déroulement illustré ci-dessous est le suivant :

1. Alice prépare un message pour Bob.
2. Alice utilise la clé publique de Bob pour chiffrer le message – elle s'assure ainsi que seul Bob – en utilisant sa clé privée – pourra le lire.
3. Alice envoie le message à Bob.
4. Bob utilise sa clé privée pour déchiffrer le message.



Mesures à envisager

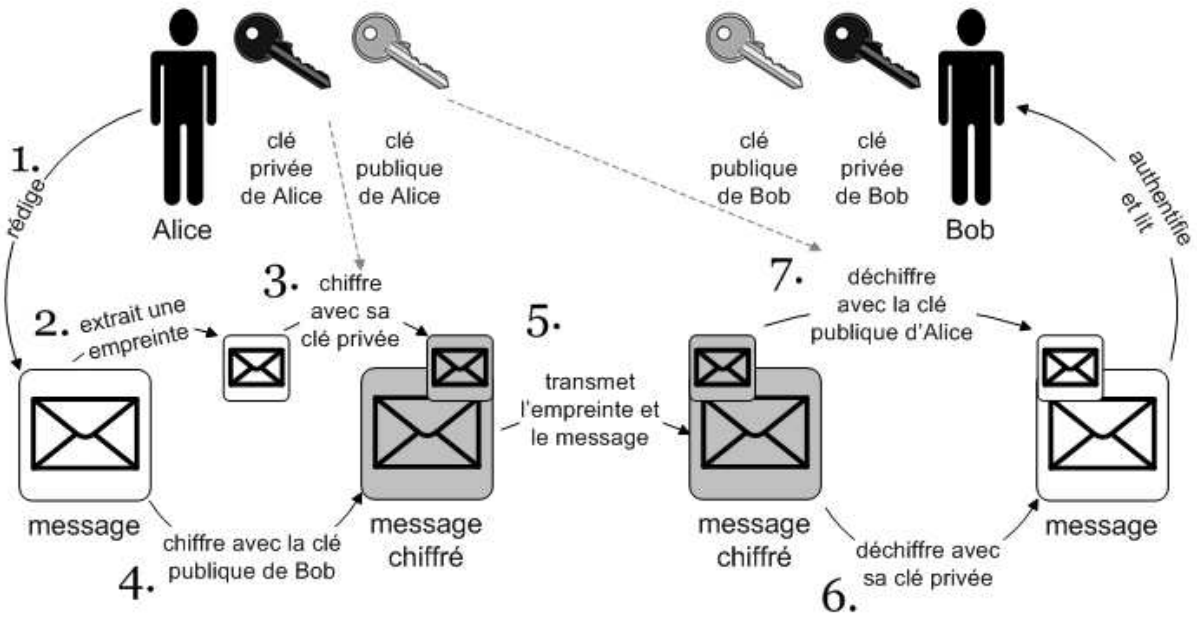
- Il faut déterminer quel type de chiffrement est le plus adéquat, suivant la sensibilité des données et les tiers avec qui l'organisation traite.
- Si le chiffrement symétrique est utilisé, il faut définir un protocole sûr pour la transmission de la clé (l'email, par exemple, n'est pas sûr).
- Si on choisit le chiffrement asymétrique, il faut mettre en place un mécanisme le chiffrement des messages. Il convient de le coupler avec la signature des messages (cf. section C.3 – Signature des messages).

C.3 Signature des messages

En chiffrant un message (cf. section C.2 – Chiffrement des messages), il est possible de s'assurer que seule la personne en possession de la clé nécessaire au déchiffrement sera à même de lire le message. Il peut également être nécessaire que le destinataire du message soit en mesure de s'assurer que l'expéditeur est bien celui qu'il prétend être. En signant le message, l'expéditeur peut transmettre cette information de manière sûre.

Cette action est habituellement effectuée préalablement au chiffrement du message selon le protocole suivant :

1. Alice rédige un message.
2. Alice extrait une empreinte de ce message. Cette empreinte sert de signature au message.
3. Alice signe cette empreinte avec sa clé privée.
4. Elle chiffre ensuite le message selon la procédure décrite plus haut.
5. Alice transmet l'empreinte et le message à Bob.
6. Bob déchiffre le message.
7. Il vérifie ensuite l'empreinte avec la clé publique d'Alice et s'assure ainsi qu'elle est bien l'expéditrice du message.



Mesures à envisager

- Les collaborateurs sont sensibilisés aux situations dans lesquelles une communication doit être signée et chiffrée.
- Les collaborateurs connaissent la manière de chiffrer et de signer les messages.

C.4 Transmission des supports de données

La transmission des supports de données mobiles est un problème délicat puisque cela implique qu'une partie des données sort de manière physique de l'organisation et est transporté vers un autre lieu. Il est essentiel que ces supports soient protégés durant leur transport afin d'éviter qu'en cas de perte ou – plus grave – de vol, les données deviennent accessibles. Plus les données contenues sur les supports mobiles sont sensibles, plus la transmission doit être sécurisée.

Mesures à envisager

- Les destinataires à qui sont remis les supports peuvent être authentifiés de manière sûre.
- La mise sous pli des supports avant la transmission est effectuée de manière sécurisée.
- Si nécessaire, les supports mobiles sont chiffrés.
- Un protocole de transport est défini. Par exemple, les supports peuvent être transportés dans des valises fermées à clé.
- Le principe des quatre yeux permet d'assurer que la remise et la réception des données est effectuée correctement. Par exemple, la personne qui remet les données et celle qui les reçoit combinent leur mots de passe respectifs pour accéder aux données.

C.5 Journalisation des transferts

L'envoi de données via le réseau Internet et la transmission de supports mobiles peuvent être protocolés et enregistrés dans un journal. Ce mécanisme de journalisation permet de tracer les expéditeurs et les destinataires des données et la manière dont les supports ont été transmis. Dans des cas d'abus, de mauvaise utilisation ou d'action malencontreuse, une certaine quantité d'informations peut ainsi être retrouvée et permet de retracer le trajet des données depuis l'expéditeur jusqu'au moment où le problème est survenu.

Les exigences introduites à la section B.2 – Journalisation s'appliquent également pour les journalisations de transfert.

Mesures à envisager

- Il faut définir une journalisation très précise qui recense les expéditeurs, les destinataires, le trajet effectué et tous les points intéressants du trajet.

- Il est préférable de confier toujours les transferts de supports aux mêmes collaborateurs.

- Il est nécessaire d'appliquer le principe de proportionnalité à la journalisation des transferts suivant leur ampleur, la durée, etc.

THÉMATIQUE D. LE DROIT D'ACCÈS

Les personnes concernées sont les personnes dont les données personnelles sont présentes dans les systèmes. Chacun a le droit de savoir si des données personnelles le concernant existent. Si de telles données sont présentes, la personne concernée peut demander leur destruction ou leur rectification si ces données s'avèrent erronées.

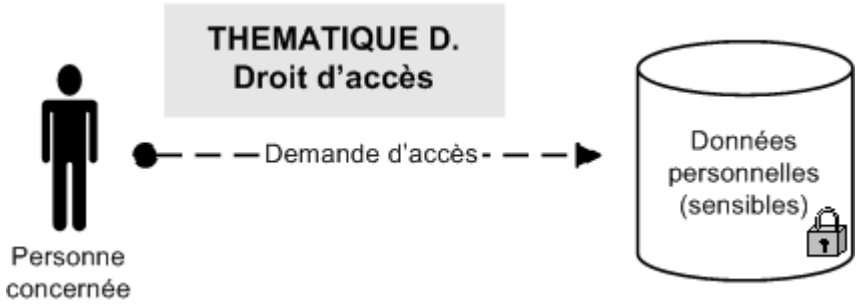


Schéma D. Le droit d'accès

Dans cette thématique, nous développons les points suivants :

D.1 Comment assurer que les personnes concernées puissent faire valoir leur droit ?
D.2 Comment assurer la reproductibilité des procédures d'exécution du droit d'accès ?

D.1 Droit des personnes concernées

Les personnes concernées ont le droit d'accéder à leurs données et d'en demander la rectification, le blocage ou la destruction. L'organisation doit être en mesure de recevoir et de traiter de manière appropriée ces demandes. Les différentes opérations demandées par les personnes concernées doivent ensuite être répercutées dans le système. Le mécanisme de recherche des données personnelles doit être efficace. Les opérations doivent également pouvoir être effectuée avec succès. Ainsi, par exemple, si une personne demande la destruction de ses données, le système doit garantir que la totalité des données sont effacées par l'opération.

Mesures à envisager

- Une information claire pour les personnes est disponible. Elle permet à chacun de connaître ses droits.
- Une procédure pour les demandes d'accès est mise en place et connue des collaborateurs.
- Le système est équipé d'un mécanisme de recherche fiable.
- Les procédures de modification, de rectification, de blocage et de destruction sont documentées et fiables.
- Tous les traitements sont journalisées.

D.2 Reproductibilité des procédures

La procédure qui permet d'exécuter le droit d'accès des personnes concernées doit être clairement définie et reproductible. Si le mécanisme est préprogrammé dans le système qui permet de traiter les données, tous les collaborateurs auront la possibilité d'effectuer les rectifications, verrouillages ou destructions de données demandées par les personnes concernées. Un mécanisme préprogrammé est également bénéfique lors d'un contrôle effectué par une autorité de surveillance puisqu'il démontre que le droit d'accès est applicable.

Mesures à envisager

- La procédure d'exécution du droit d'accès est préprogrammée dans le système.
- Tous les collaborateurs utilisent la même procédure.
- L'autorité de surveillance peut effectuer son travail si nécessaire en testant la procédure intégrée au système.

OUTILS EXISTANTS

Certains outils existent pour optimiser la mise en œuvre des mesures techniques et organisationnelles.

La grille d'évaluation

Le Préposé fédéral à la protection des données et à la transparence met à disposition une grille d'évaluation qui permet d'anticiper les risques en ciblant très tôt dans le développement d'un nouveau projet les points problématiques en matière de protection des données.

La grille d'évaluation est disponible sur le site internet (Protection des données - Commerce et économie - Entreprises) du PFPDT.

Le règlement de traitement

Le règlement de traitement est un outil prévu par le droit suisse qui aide à la définition de mesures techniques et organisationnelles appropriées. Le but d'un tel règlement est d'assurer une transparence nécessaire lors de l'élaboration et la gestion d'une collection de données personnelles (fichier). Il permet de réunir les différentes documentations qui ont été préparées par les différentes unités en charge du projet et de centraliser ainsi les informations. Les responsables de la protection des données et les exploitants du système peuvent bénéficier d'une documentation complète qui leur permet de repérer les bonnes pratiques et de les appliquer.

Le règlement de traitement doit être élaboré par le maître du fichier.

Contenu du règlement

Si le maître du fichier est une personne privée, le règlement de traitement doit contenir d'une part la description de l'organisation interne et celle des procédures de traitements et de contrôle des données, et d'autre part, toute la documentation relative à la planification, à l'élaboration et à la gestion des moyens informatiques, tant les logiciels que le matériel.

Si le maître du fichier est un organe fédéral, le règlement de traitement est requis seulement dans les cas où (1) le fichier contient des données sensibles ou des profils de la personnalité, (2) le fichier est utilisé par plusieurs organes fédéraux, (3) le fichier est accessibles à des tiers, tels que les cantons, les autorités étrangères, des organisations internationales ou des personnes privées, et (4) le fichier est interconnecté avec d'autres fichiers.

Le contenu du règlement de traitement pour les organes fédéraux est défini de manière très précise.

1. L'organisation interne – les opérations effectuées par le système et l'organisation structurelle – doit être documentée avec la mention des différentes responsabilités (protection des données, maître du fichier, etc.).
2. Les documents relatifs à la planification, l'élaboration et la gestion des moyens informatiques doivent être conçus de manière transparente.
3. Un récapitulatif des mesures techniques et organisationnelles permet de déterminer quelles sont les mesures déjà en place.
4. L'origine des données et les buts des traitements doivent être décrits.
5. L'obligation de déclarer est décrite par les indications nécessaires.
6. L'ensemble des champs de données est défini. Une matrice d'accès indique quelles unités organisationnelles et quelles personnes ont accès aux données.
7. Les mesures pour l'application du droit d'accès sont décrites.
8. La configuration des moyens informatiques mentionne tous les logiciels ainsi que le matériel utilisé.

Le règlement de traitement doit être mis à jour régulièrement et mis à disposition des autres organes concernés.

Afin d'aider à l'élaboration d'un règlement de traitement, le PFPDT a publié sur son site le document « Que doit contenir un règlement de traitement ? »[2].

CONSIDÉRATIONS FINALES

L'application des mesures techniques et organisationnelles présentées dans ce guide permet d'assurer une protection des données appropriée. Toutefois, il est nécessaire de toujours prendre en compte le contexte global dans lequel s'inscrit un projet, sa sensibilité, la quantité de données nécessaires, etc.

La responsabilité de la protection des données incombe au maître du fichier. En abordant ce problème le plus tôt possible dans l'élaboration du projet, il lui sera possible de minimiser les risques.

[2] www.leprepose.ch > Documentation > Protection des données > Brochures > Mesures techniques et organisationnelles